CLAIMS

What is claimed is:

1. An apparatus comprising:

at least one data bit generator to generate a first, second and third plurality of data bits; and

a combiner function, coupled to the at least one data bit generator, including a network of shuffle units, to combine the third plurality of data bits, using the first and second plurality of data bits as first input data bits and control signals respectively of the network of shuffle units.

2. The apparatus of claim 1, wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops in a topological manner to control selective output of one of the first and second state values based on a corresponding one of said second plurality of data bits.

3. The apparatus of claim 2, wherein said plurality of selectors are coupled to said first and second flip-flops of the shuffle unit in a topological manner that results in the first state value of the shuffle unit being output when the corresponding one of said second plurality of data bits is in a first state, and the second state value of the shuffle unit being output when the corresponding one of said second plurality of data bits is in a second state.

4. The apparatus of claim 2, wherein said plurality of the selectors are further coupled to said first and second flip-flops of the shuffle unit to control selective modification of the first and second state values stored in said first and second flip-flops of the shuffle unit based on the same corresponding one of said second plurality of data bits.

5. The apparatus of claim 4, wherein said plurality of selectors are coupled to said first and second flip-flops of the shuffle unit in a topological manner that results in the first state value being output and the first and second flip-flops of the shuffle unit to store said second state value and a second input data bit respectively when the corresponding one of said second plurality of data bits is in a first state, and the second state value being output and the first and second flip-flops of the shuffle unit to store the second input data bit and said first state value respectively when the corresponding one of said second plurality of data bits is in a second state.

6. The apparatus of claim 5, wherein the second input value is a selected one of an output data bit of an immediately preceding shuffle unit and an output data bit generated from said first plurality of data bits.

7. The apparatus of claim 1, wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops to control modification of the first and second state values based on a corresponding one of said second plurality of data bits.

8. The apparatus of claim 7, wherein said plurality of selectors are coupled to the first and second flip-flops in a topological manner that results in the first and second flip-flops of the shuffle unit to store said second state value and a second input data bit respectively when the corresponding one of said second plurality of data bits is in a first state, and the first and second flip-flops of the shuffle unit to store the second input data bit and said first state value respectively when the corresponding one of said second plurality of data bits is in a second state.

9. The apparatus of claim 8, wherein the shuffle units are serially coupled to each other with a first of the shuffle unit serially coupled to the first XOR gate, and said second input data bit is a selected one of an output bit of an immediately preceding shuffle unit and an output bit generated from the first plurality of data bits.

10. The apparatus of claim 1, wherein the combiner function further comprises an exclusive-OR gate to combine the first plurality of data bits for the network of shuffle units.

11. The apparatus of claim 1, wherein the combiner function further comprises an exclusive-OR gate to combine the third plurality of data bits using an output bit of the network of shuffle units.

12. The apparatus of claim 11, wherein the apparatus further comprises a register coupled to the XOR gate to store a cipher key and allow the stored cipher key to be periodically modified by the output of the exclusive-OR gate.

13. The apparatus of claim 12, wherein the apparatus further comprises a function block coupled to the register to successively transform the modified cipher key, and a mapping block coupled to the register to generate a pseudo random bit sequence based on the successive transformed states of the modified random number.

14. The apparatus of claim 1, wherein the at least one data bit generator comprises a plurality of LFSRs to generate said first, second, and third plurality of data bits.

15. The apparatus of claim 1, wherein the apparatus is a stream cipher.

16. An apparatus comprising:

a first XOR gate to receive a first plurality of data bits and combine them into a second data bit;

a network of shuffle units, coupled to the first XOR gate, to output a third data bit by shuffling and propagating the second data bit through the network of shuffle units under the control of a four plurality of data bits; and

a second XOR gate coupled to the network of shuffle units to combine a fifth plurality of data bits using the third data bit.

17. The apparatus of claim 16, wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops to control selective output of one of the first and second state values based on a corresponding one of said fourth plurality of data bits.

16. The apparatus of claim 15, wherein said plurality of selectors are coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in the first state value of the shuffle unit being output when the corresponding one of said fourth plurality of data bits is in a first state, and the second state value of the shuffle unit being output when the corresponding one of said fourth plurality of data bits is in a second state.

17. The apparatus of claim 16, wherein said plurality of the selectors are further coupled to the first and second flip-flops to control selective modification of the first and second state values stored in the first and second flip-flops of the shuffle unit based on the same corresponding one of said fourth plurality of data bits.

18. The apparatus of claim 17, wherein said plurality of selectors are coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in the first state value being output and the first and second flip-flops of the shuffle unit to store said second state value and a sixth data bit respectively when the corresponding one of said fourth plurality of data bits is in a first state, and the second state value being output and the first and second flip-flops of the shuffle unit to store the sixth data bit and said first state value respectively when the corresponding one of said fourth plurality of data bits is in a second state.

19. The apparatus of claim 18, wherein the shuffle units are serially coupled to each other with a first of the shuffle unit serially coupled to the first XOR gate, and said sixth data bit is a selected one of said second data bit and the output of an immediately preceding shuffle unit.

20. The apparatus of claim 14, wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and a plurality of selectors coupled to the first and second flip-flops to control modification of the first and second state values based on a corresponding one of said fourth plurality of data bits.

21. The apparatus of claim 20, wherein said plurality of selectors are coupled to the first and second flip-flops of the shuffle unit in a topological manner that results in the first and second flip-flops of the shuffle unit to store said second state value and a sixth data bit respectively when the corresponding one of said fourth plurality of data bits is in a first state, and the first and second flip-flops of the shuffle unit to store the sixth data bit and said first state value respectively when the corresponding one of said fourth plurality of data bits is in a second state.

22. The apparatus of claim 21, wherein the shuffle units are serially coupled to each other with a first of the shuffle unit serially coupled to the first XOR gate, and said sixth data bit is a selected one of said second data bit and the output of an immediately preceding shuffle unit.

23. The apparatus of claim 14, wherein the apparatus further comprises a register coupled to the second exclusive-OR gate to store a value to be periodically modified using the result of said combination of the fifth plurality of data bits.

24. The apparatus of claim 23, wherein the apparatus further comprises a function block coupled to the register to successively transform a modified version of

the stored value, and a mapping block coupled to register to generate a pseudo random bit sequence based on the successively transformed states of the modified value.

25. The apparatus of claim 14, wherein the apparatus is a stream cipher.

26. A method comprising:

generating a first, second and third plurality of data bits; and

shuffling and propagating a fourth data bit generated from the first plurality of data bits, under the control of the second plurality of data bits, to output a fifth data bit to combine the third plurality of data bits.

27. The method of claim 26, wherein the fourth data bit is serially shuffle and propagated, and at each stage, a first state value is output when the corresponding one of said second plurality of data bits is in a first state, and a second state value is output when the corresponding one of said second plurality of data bits is in a second state.

28. The method of claim 26, wherein the fourth data bit is serially shuffle and propagated, and at each stage, a first of the state values is replaced by an input value, and shuffled, when the corresponding one of said second plurality of data bits is in a first state, and a second of the state values is replaced by the input value, and shuffled, when the corresponding one of said second plurality of data bits is in a second state.